Como mantener seguro el ordenador de tu casa

Índice

El coste mundial de los delitos cometidos en Internet alcanza los 81.282 millones de euros anuales.

Una cantidad que sobrepasa el mercado negro global de la marihuana, la cocaína y la heroína.[1]

Este curso busca responder las siguientes tres preguntas:

- ¿Cómo evitar que te roben las claves bancarias?
- ¿Cómo evitar que otro use tu wifi?
- ¿Cómo evitar que otro tome el control de tu ordenador?

Como evitar que te roben las claves bancarias

En 2010, un 4 % de los internautas españoles perdió dinero por ataques de 'phishing' u otras técnicas para el uso fraudulento de las tarjetas de crédito. [2]

Consideraciones previas

En su mayor parte, un ordenador se usa para navegar por Internet, acceder al correo electrónico y/o descargar vídeos, música o programas de utilidad.

Estas actividades pueden provocar que el equipo desde el que se realizan sea "infectado" por un virus, con consecuencias que pueden llegar a ser extremadamente perjudiciales.

Situaciones, potencialmente, de ALTO RIESGO.

Más en concreto, una actividad cada vez más cotidiana es acceder a los sitios web de los Bancos, para gestionar los recursos allí depositados.

Otra actividad habitual es pagar recibos, entradas, impuestos, etc., o incluso realizar operaciones más complejas.

Un virus potente podría hacer llegar nuestros datos identificativos (número de cuenta y contraseña, por ejemplo) a manos indeseables.

Una solución

Para evitar problemas, una excelente solución es utilizar el

sistema LPS (una distribución de Linux)

cuya fácil implementación se describe a continuación.

El sistema LPS permite acceder al banco por internet usando únicamente la información del CD donde LPS reside, una información que sabemos que está libre de virus.

Utilizando LPS evitamos la necesidad de usar la información del ordenador donde puede estar escondido un virus.

Creación de un CD de arranque con el "sistema LPS"

Previo importante: será necesario grabar un CD cada vez que esté disponible una versión nueva del "sistema LPS", para así contar con las más recientes actualizaciones de seguridad. Se recomienda hacerlo cada tres o cuatro meses.

Descarga del software necesario

Acceder a

http://www.spi.dod.mil/lipose.htm

y descargar el archivo *.iso* de la ultima versión del sistema LPS.

Por ejemplo, buscar en la página y pinchar en el enlace,

"Download the LPS-Public ISO image, version 1.5.7 (5 March 2015)"

Guardar el archivo en el ordenador.

Grabación del "sistema LPS" en un CD

Insertar un CD en blanco en la unidad que corresponda.

Utilizando el "Explorador de Windows", acceder al archivo guardado en el paso anterior, y hacer clic en él con el botón derecho. Seleccionar "Grabar imagen de disco".

En el cuadro de diálogo que aparecerá:

- activar "Comprobar disco después de grabar", y
- hacer clic en "[Grabar]"

nota importante: al usar programas de grabación de CDs, se deberá seleccionar la opción *"Grabación de archivos ISO"* (o equivalente), pues si se realizara la grabación utilizando la opción *"Grabación de archivos de datos"* (o equivalente) no se generaría un disco de arranque, por lo que el "sistema LPS" no funcionaría.

Confirmación de una grabación correcta.

Una vez terminada la grabación, mediante el "Explorador de Windows", acceder al contenido del CD.

Se habrá conseguido una correcta grabación si aparecen (entre otros) los siguientes ficheros:

- **boot** (boot.cat),

- **initrd**.

Si sólo contiene el archivo "LPS-xxx_public.iso", el proceso no se realizó correctamente (posiblemente por no utilizar la opción "Grabación de archivos ISO" (o equivalente)).

Uso del sistema LPS

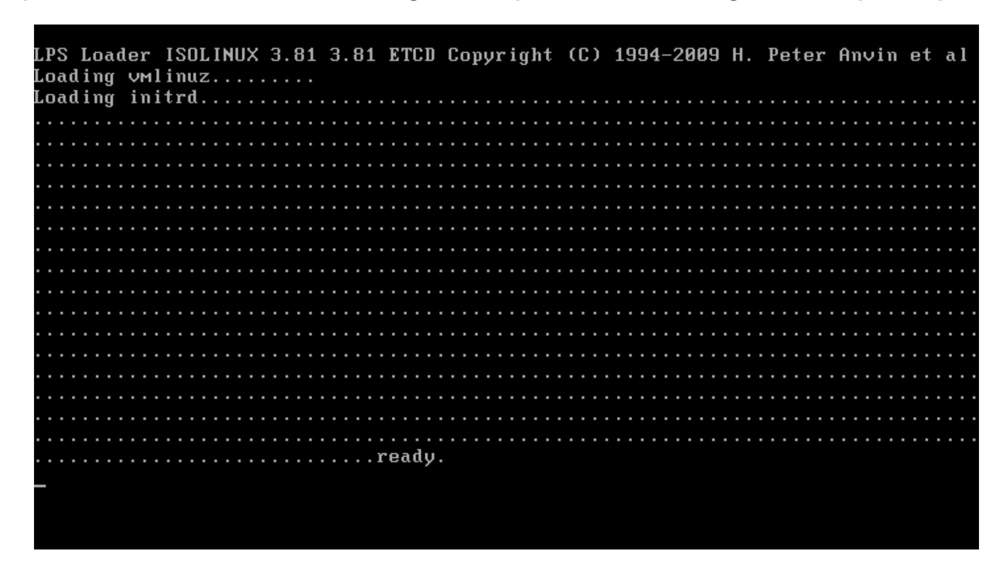
Introducir el CD recién creado en la unidad correspondiente.

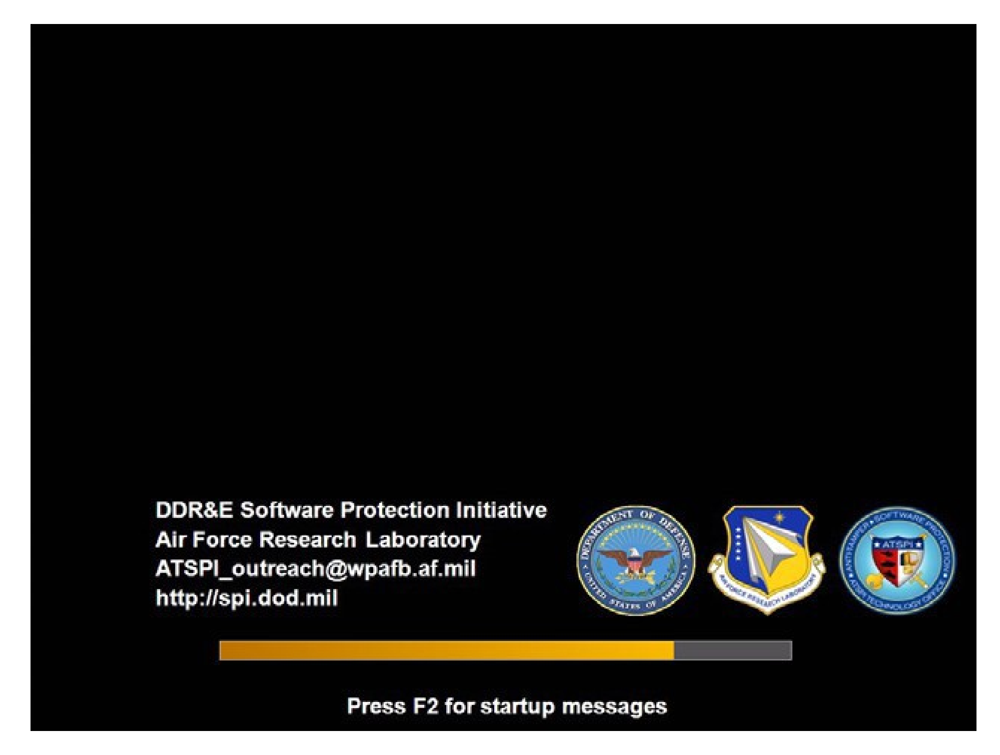
Reiniciar el equipo.

Este deberá arrancar utilizando el CD del "sistema LPS".

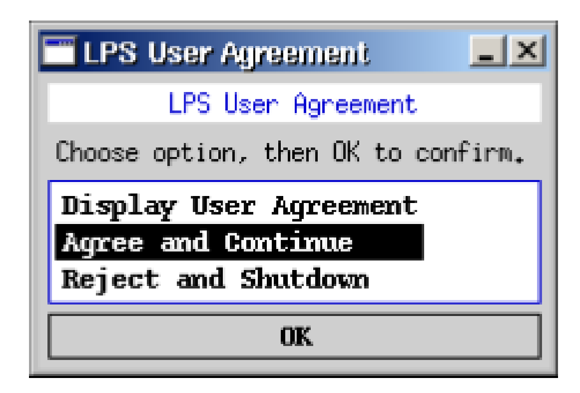
nota: si no fuera así, reiniciar de nuevo y preprarar la BIOS del equipo para que arranque desde CD.

Esperar a que el "sistema LPS" se cargue. El proceso de carga es el que aquí se muestra:





Aceptar las condiciones de uso:



Escritorio del "sistema LPS":

Para un acceso seguro a Internet utilizar Firefox (cuyo icono se encontrará arriba a la izquierda):

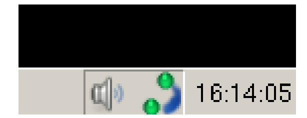


Se recomienda su uso únicamente para el acceso a la páginas web de los bancos o para actuaciones en las que sea necesario introducir datos de tarjetas de débito/crédito u otros datos sensibles.

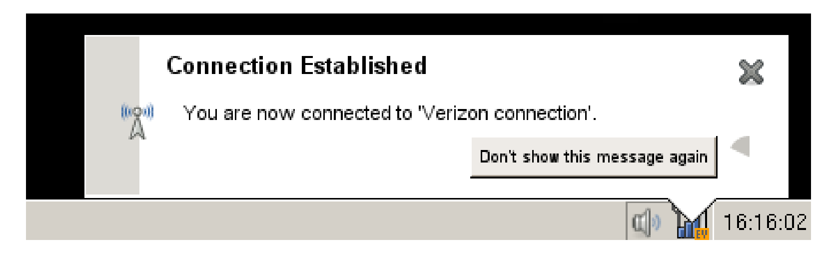
Conectarse a Internet desde el "sistema LPS"

Si el ordenador está conectado **por cable** a un router con una conexión activa a Internet, esta se establecerá de forma automática:

Así, se podrá observar, en la esquina inferior derecha, lo siguiente:



y durante unos segundos:



Pero, en el caso de usar una **red WiFi**, se deberá establecer la conexión manualmente:

- Seleccionando la red:



- Introduciendo la contraseña correspondiente:



Tras introducir la contraseña de acceso a la red WiFi, se podrá observar:



Como evitar que otro use tu wifi

En enero de 2011, la Brigada de Investigación Tecnológica, detuvo en Valencia a un ciudadano uruguayo que accedió de forma fraudulenta al sistema informático de la Banca de Loterías y Quinielas de Uruguay, ocasionando daños valorados en más de un cuarto de millón de dólares.

La búsqueda y captura del detenido fue dificultada porque este, no había realizado el ataque desde su propia conexión a Internet sino que había utilizado una red wifi desprotegida de un ciudadano valenciano que vivía cerca de donde el detenido tenía su lugar de trabajo.[3]

1. Lo primero y fundamental, es apagar el router cuando no lo estés usando.

2. En segundo lugar debes asegurarte de que tu router se comunica con tu ordenador usando el protocolo WPA2.

Actualmente, WPA2 es el único protocolo que puede asegurarte protección.

Para comprobar que lo tienes, puedes mirar si existe una pegatina en tu router, indicando estos datos.

En caso contrario, habla con tu compañía telefónica.

3. En tercer lugar, cambia la contraseña

No uses la contraseña que te ha dado tu compañía de teléfono.

Elige una contraseña que sea difícil de adivinar.

- No usar palabras que se puedan encontrar en un diccionario
- Usar una longitud de contraseña de 8 dígitos al menos.
- Combinar mayúsculas, minúsculas, números y símbolos.

Para que la contraseña sea fácil de recordar, se puede utilizar el método de la frase.

E1Idlm,dcnnqa

“En un lugar de la mancha, de cuyo nombre no quiero acordarme”

Como evitar que otro tome el control de tu ordenador

Uno de cada tres internautas españoles , ha sido infectado por un virus.[4]

¿Por qué querría alguien tomar el control de tu ordenador?

Hay varias formas en las que el creador de un programa malicioso puede obtener un beneficio económico.

Las más comunes son:

- Robar información sensible del ordenador infectado, como datos personales, contraseñas, datos bancarios…
- Crear una red de ordenadores infectados (red zombi o botnet) para que el atacante pueda manipularlos todos simultáneamente.

Y vender estos servicios a entidades sin escrúpulos que puedan realizar acciones poco legítimas como

  - el envío de SPAM,
  - envío de mensajes de phishing,
  - realizar ataques de denegación de servicio contra empresas o gobiernos, ...

- Vender falsas soluciones de seguridad que no realizan las acciones que afirman hacer.

Por ejemplo, falsos antivirus que muestran mensajes con publicidad informando de que el ordenador está infectado.

Cuando en realidad no es así, la infección que tiene el usuario es el falso antivirus.

Proteger un ordenador hoy en día es como proteger un castillo en la edad media

1 No confiar en extraños

No abrir las puertas de tu castillo a cualquiera.

No te fíes de e-mails de desconocidos ni de lo que te pida una páginas web. Ignora las peticiones de “haz clic aquí”.

2 Utilizar siempre los mínimos permisos

Internet es un territorio que esta fuera de tu castillo, es peligroso y esta lleno de atacantes y enemigos.

Pero Internet esta lleno de cosas útiles y que necesitas para la vida en el castillo.

Sin embargo, no necesitas salir tu mismo del castillo, puedes enviar a un mensajero o un criado, de forma que, si es atrapado por tus enemigos, no pueda ser utilizado para entrar en tu castillo.

En el caso de tu ordenador, el mensajero se llama “usuario sin permisos de administración”.

3 Proteger las contraseñas

Has ordenado a tus guardias que dejen entrar en el castillo a toda persona que sepa una contraseña que has elegido tú.

Si esta contraseña es muy fácilmente adivinable, cualquiera puede entrar en tu castillo y de nada te sirve tener un foso con pirañas y pagar a un montón de guardias.

4 Mantener actualizado todos los programas.

Imagina que tu ordenador es un castillo.

Cuando se construye el castillo las paredes son sólidas y resistentes pero con el paso del tiempo se van descubriendo agujeros por los que puede entrar un intruso.

Lo mismo pasa con los programas, se van descubriendo agujeros que son tapadas por las actualizaciones.

5 Un antivirus

El antivirus son los guardias que tienes apostados en las murallas de tu castillo y en el interior.

Matan a todos los intrusos y atacantes que son capaces de detectar.

6 Un cortafuegos

El cortafuegos cumple la misma función que un foso con pirañas y un puente levadizo en un castillo.

Solo permite entrar y salir a las personas que tú quieres.

No confiar en extraños

Precaución con los correos que se reciben:

"Soy tu banco y necesito tus contraseñas" No.
"Soy hacienda y quiero tu tarjeta de crédito para devolverte dinero" No.
"Soy facefook y quiero tu usuario y password" No.
"Soy Bill Gates y quiero compartir mi fortuna contigo". No.
No, no, no y no.

Ni tu banco, ni hacienda, ni facebook te van a pedir tus contraseñas. Si por alguna razón piensas que la petición es legítima, lo mejor es que busques un teléfono de contacto (por otro medio independiente) y llames a la entidad sosopechosa para confirmar que te lo han petido ellos.
Importante: Nunca uses los datos de contacto (link a pagina web, telefono) que haya en el e-mail sospechoso.

Si ves esto,

"Estimado cliente, su tarjeta de crédito ha sido bloqueada por su seguridad. Para desbloquearla acceda a xxx.tarjetago.xx y complete los datos en 24h."

Complete los siguientes datos para desbloquear su tarjeta

Introduzca el número de su tarjeta:	
Fecha de caducidad de la tarjeta: mes/año:	/
Clave Secreta de su Tarjeta (PIN que utiliza en los cajeros):	
CVV Código de Verificación de la Tarjeta: ¿Que es el CVV ?	
Tipo de Documento de Identidad:	N.I.F. (Incluyendo letra)
Número de Documento de Identidad - Excepto T. Virtual Anónima:	
Fecha de Nacimiento:	

Continuar | Borrar datos

Debes borrar el mensaje sin contestarlo.

También se recomienda ser cuidadoso con los datos personales que se dan por internet.

Si se quiere registrar o dar datos, se recomienda tener una segunda o una tercera cuenta de correo.

Y utilizar la cuenta de correo principal solo para asuntos oficiales y para compartir con gente en la que confiamos.

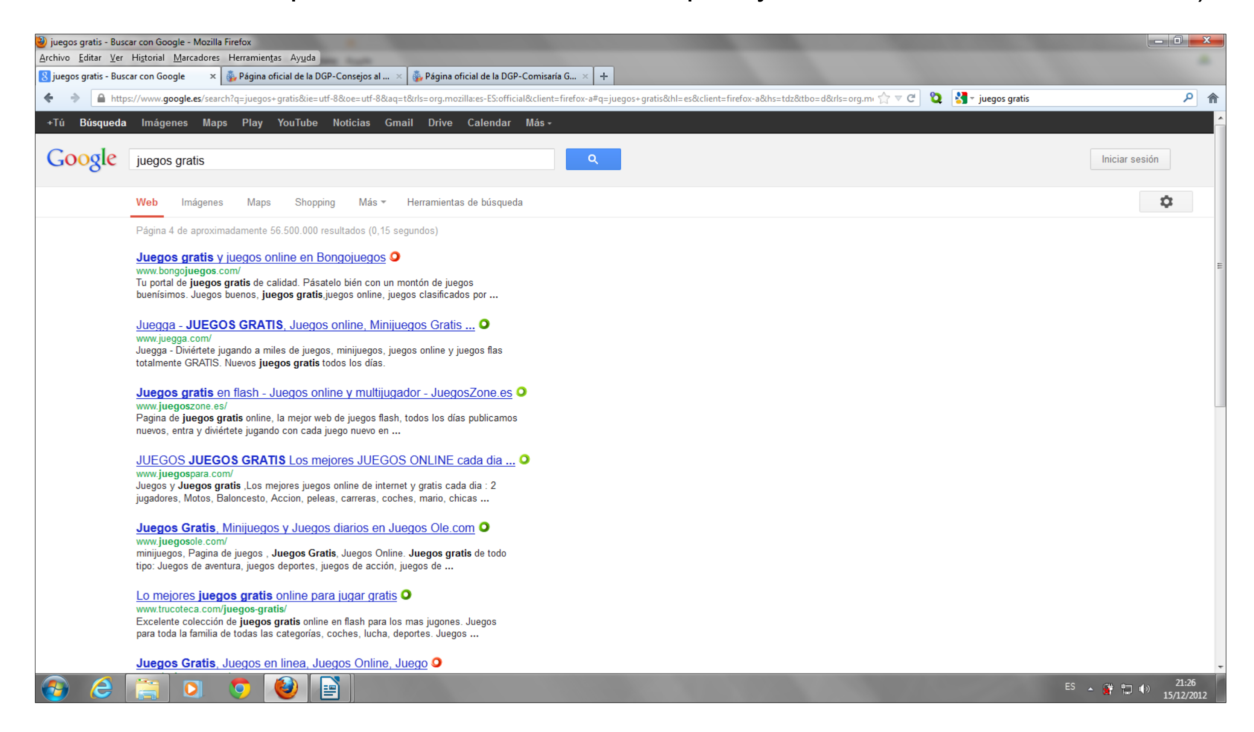
Precaución con las páginas web que se visitan

En ningún caso instales nada que te proponga una página web o un programa que no conozcas.

Algunas extensiones para navegador pueden ayudar a detectar sitios dañinos.

Por ejemplo, WOT

(También el antivirus puede incluir herramientas que ayuden a detectar sitios dañinos)



Para instalar WOT en Firefox se debe:

Ir a Herramientas → Complementos → Obtener Complementos

Buscar WOT en el cuadro de búsqueda y hacer clic en Instalar

Para instalar WOT en Chrome se debe:

Ir a Herramientas → Extensiones → Obtener Mas Extensiones

Buscar WOT en el cuadro de búsqueda y hacer clic en Añadir a Chrome

Para instalar WOT en Internet Explorer se debe:

Ir a la página oficial de WOT, http://www.mywot.com/en/download

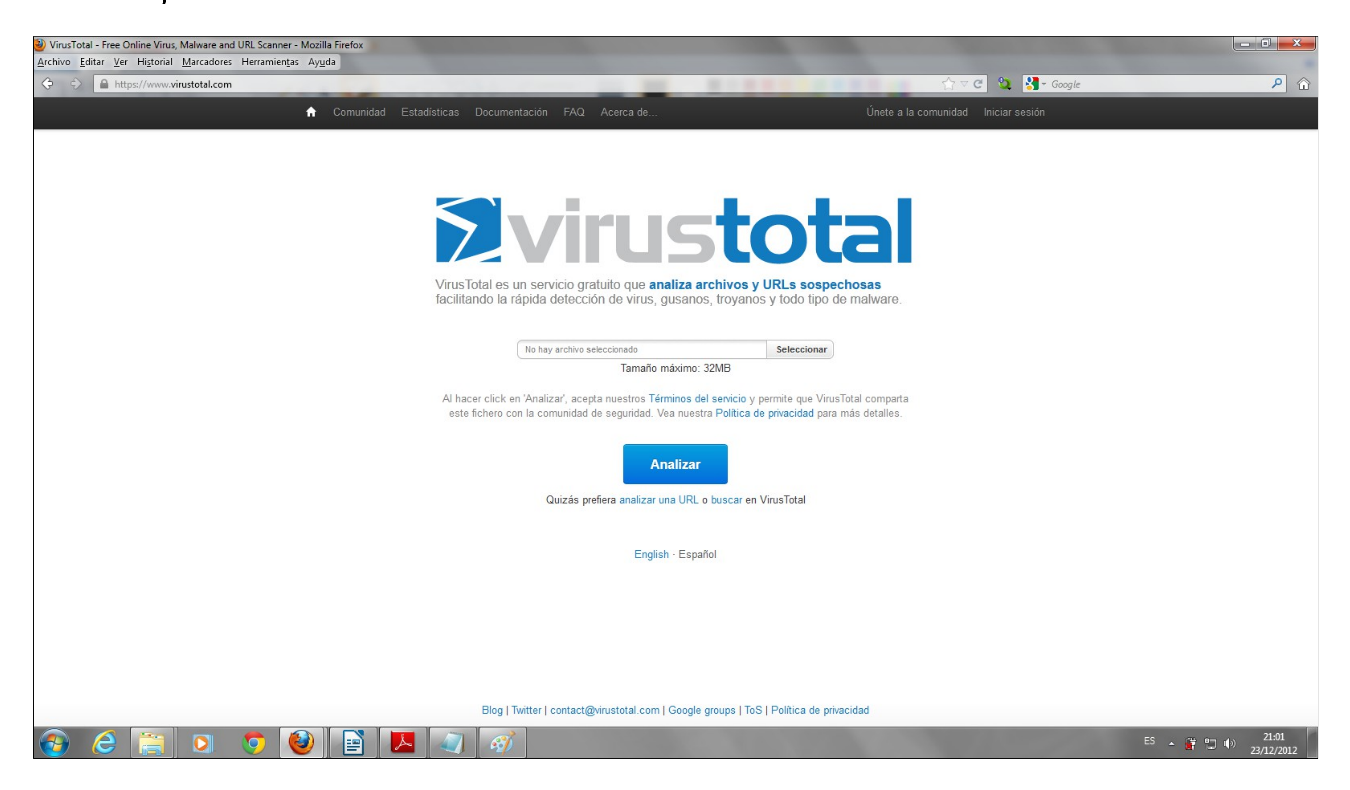
e instalarlo desde allí.

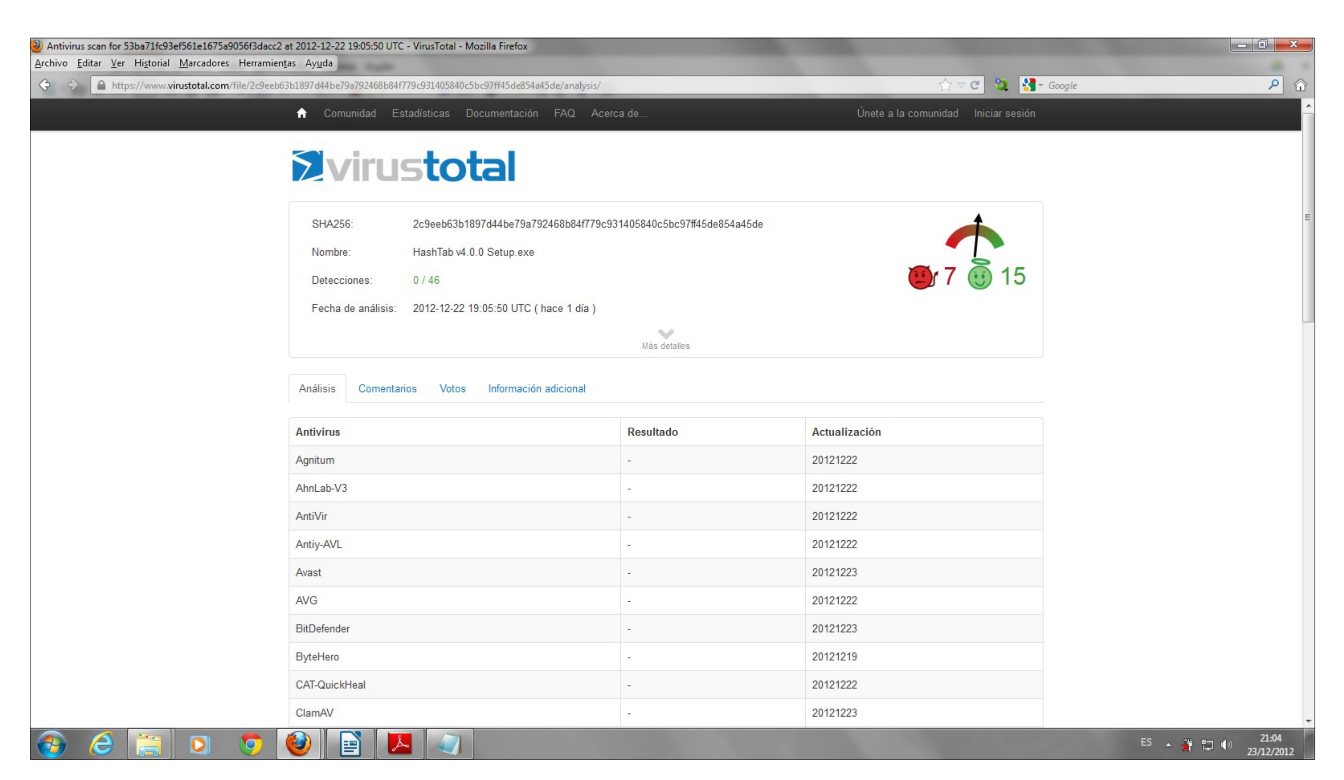
Se recomienda siempre obtener los programas o contenidos de sus respectivos sitios **oficiales**.

También se recomienda analizar los archivos descargados con un motor antivirus antes de abrirlos

Para ello, puedes usar la herramienta online Virus Total

https://www.virustotal.com/





Además,

Revisa periódicamente tus cuentas para detectar transferencias irregulares.

Consulta si tu banco tiene servicio de aviso de movimiento de cuentas por sms.

Al utilizar cajeros bancarios, tapa los números del pin que pulsas para que no puedan ser grabados con una cámara.

Utiliza una tarjeta prepago (no asociada a tu cuenta bancaria).

Utilizar siempre los mínimos permisos

Por defecto, en Windows el usuario que se crea al instalar el equipo es administrador, es decir, tienen control total sobre el equipo, puede instalar cualquier programa y modificar lo que desee.

Este usuario es muy probablemente el que estas usando.

Esto significa que si navegas como administrador y accedes a una página, ves un video o abres un pdf que contenga código malicioso (un virus), de repente estás infectado y tienes un virus que espía todos tus movimientos.

Esto es más difícil que te pase si navegas con un usuario al que previamente le has quitado los permisos para realizar cambios en el equipo.

¿Como quitarle los permisos a un usuario?

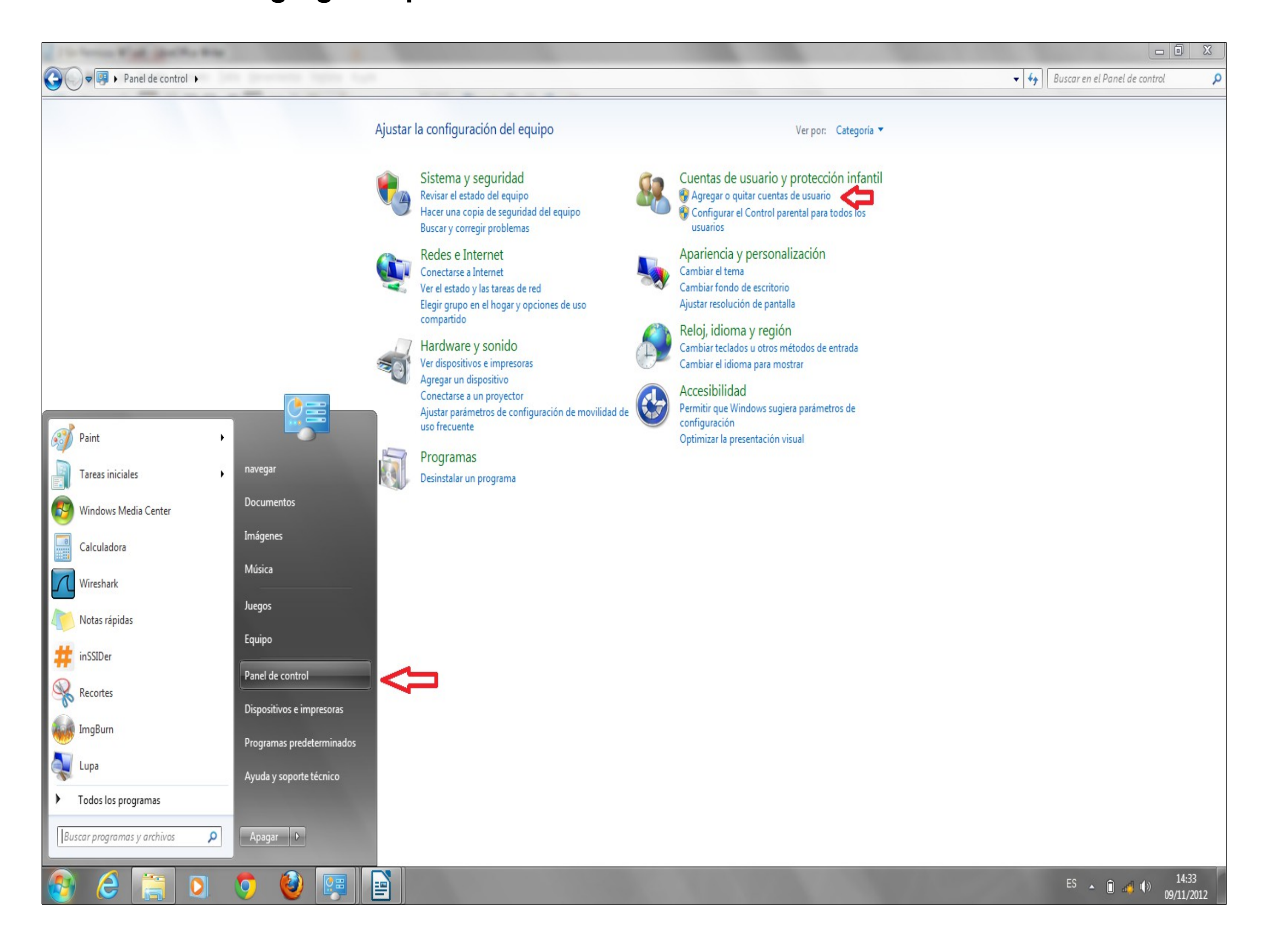
Vamos a

A. Crear un usuario nuevo, administrador, para usar solo en caso de que queramos modificar algo en el equipo.

B. Quitarle los permisos al usuario que usamos siempre

A Crear un usuario nuevo, administrador

Hacer clic en Inicio --> Panel de Control --> Cuentas de usuario
Hacer clic en “Agregar o quitar cuentas de usuario”



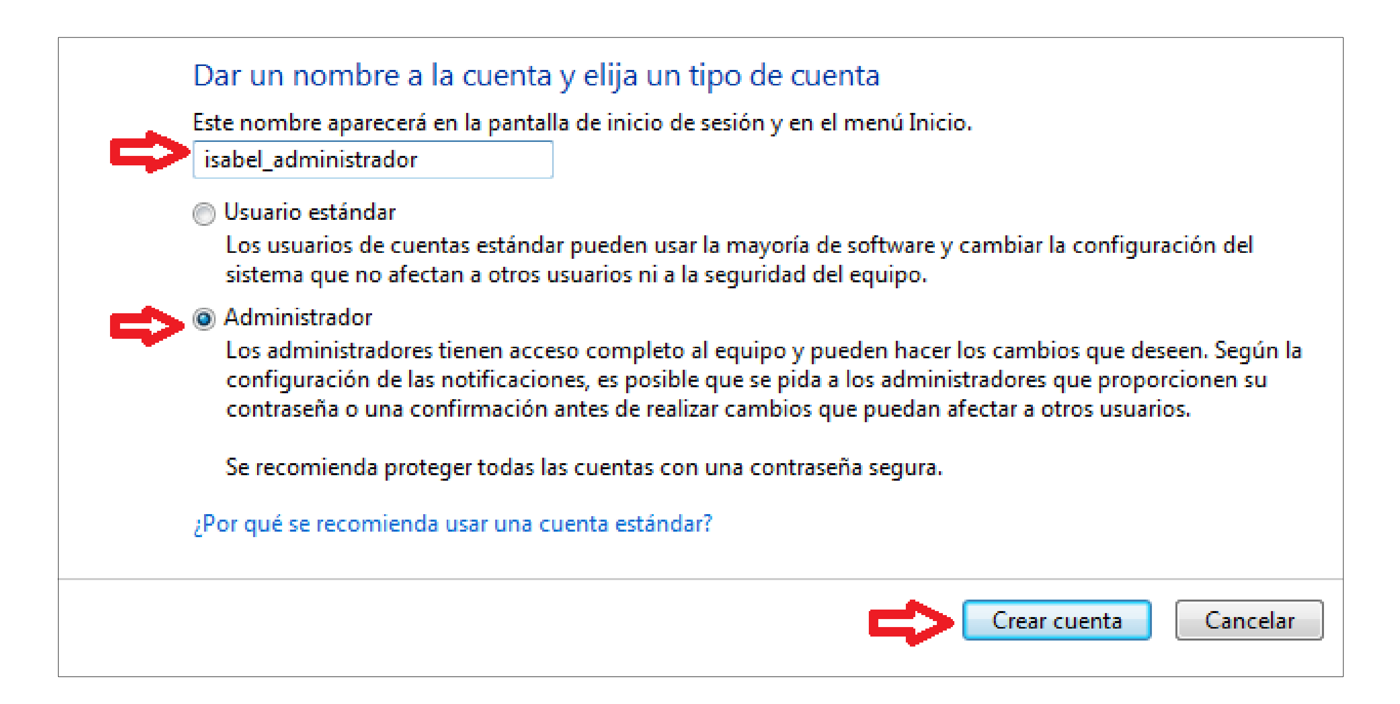
Hacer clic en *Crear una cuenta nueva*



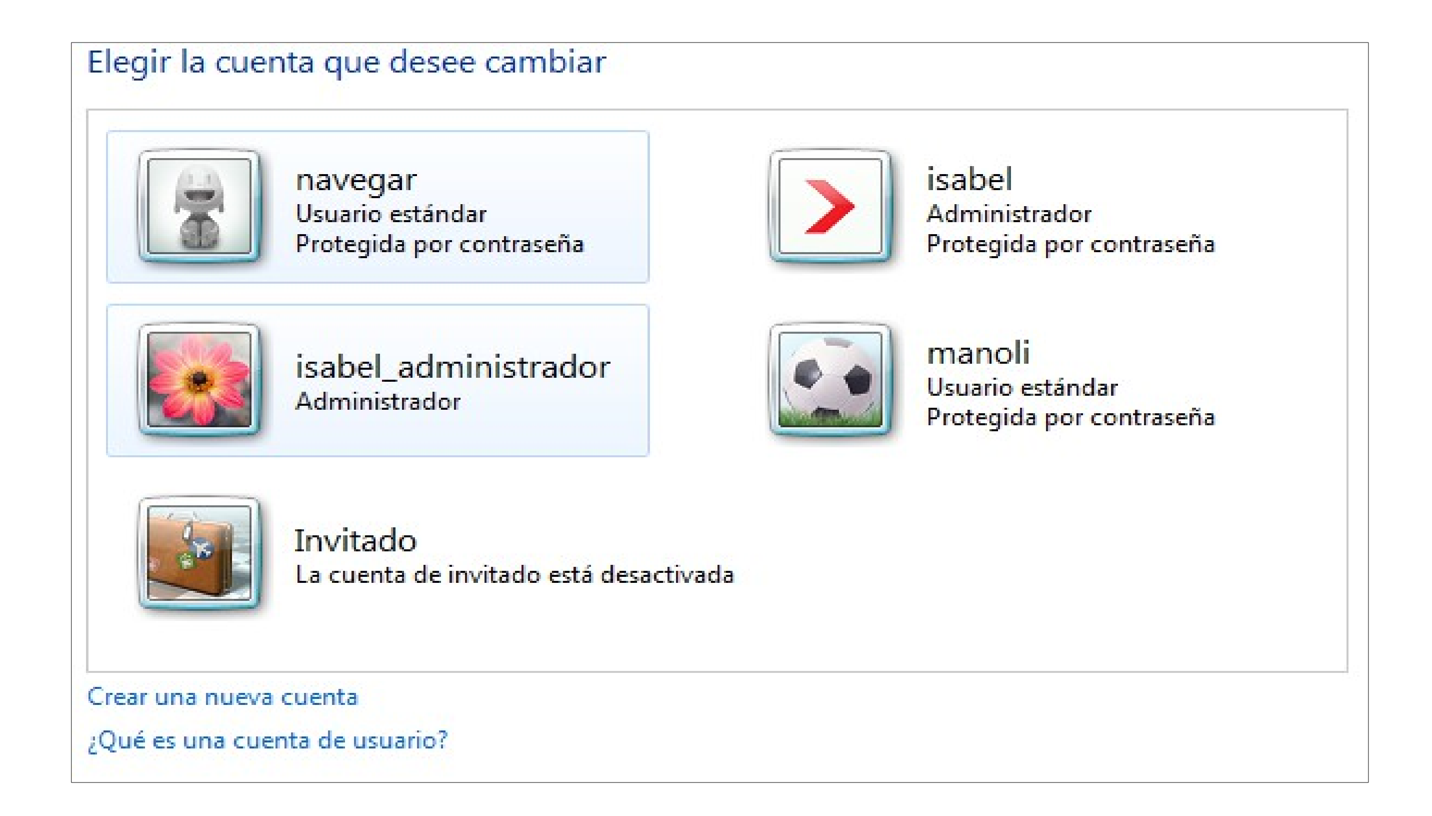
Poner un nombre a la cuenta, elegir tipo *Administrador* y pulsar en el botón *Crear cuenta*

Esta cuenta solo se debe usar para hacer cambios en el ordenador, instalar, desinstalar programas, ...

No se debe usar para navegar por internet.



Ponerle una contraseña a la cuenta

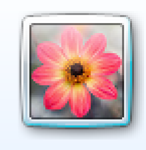


Realizar cambios en la cuenta de isabel_administrador



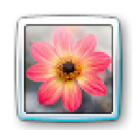
Cambiar el nombre de cuenta
Crear una contraseña
Cambiar la imagen
Configurar Control parental
Cambiar el tipo de cuenta
Eliminar la cuenta

Administrar otra cuenta



isabel_administrador
Administrador

Crear una contraseña para la cuenta de isabel_administrador



isabel_administrador
Administrador

Está creando una contraseña para isabel_administrador.

Si hace esto, isabel_administrador perderá todos los archivos EFS cifrados, certificados personales y contraseñas almacenadas para los sitios web o los recursos de red.

Para evitar pérdida de datos en el futuro, solicite a isabel_administrador que cree un disquete para restablecer contraseñas.



Nueva contraseña
Confirmar contraseña nueva

Si la contraseña contiene mayúsculas, no se olvide de escribirlas de la misma forma.
Cómo crear una contraseña segura

Escriba un indicio de contraseña

El indicio de contraseña será visible para todos los usuarios que utilicen este equipo.
¿Qué es un indicio de contraseña?

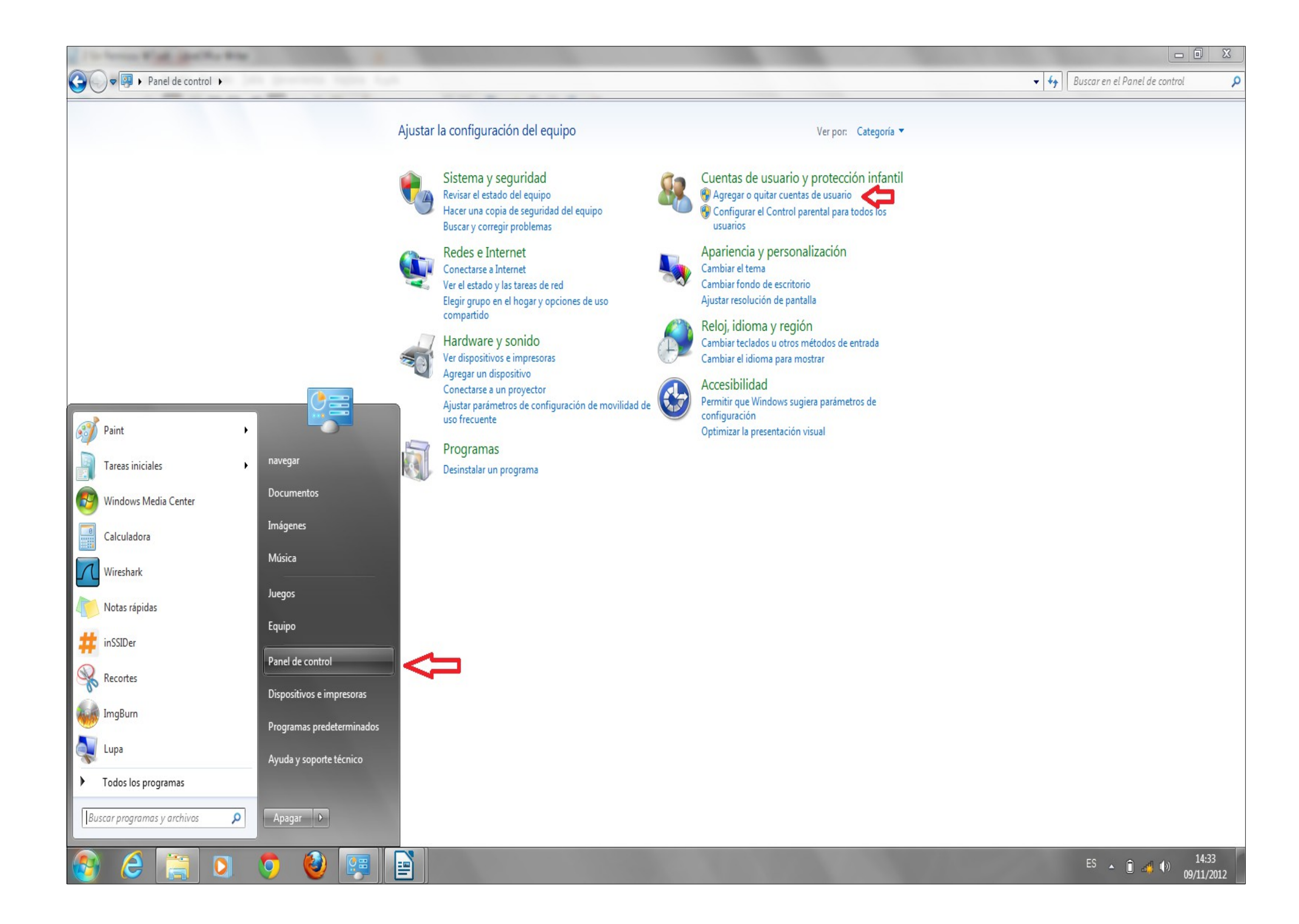


Crear contraseña | Cancelar

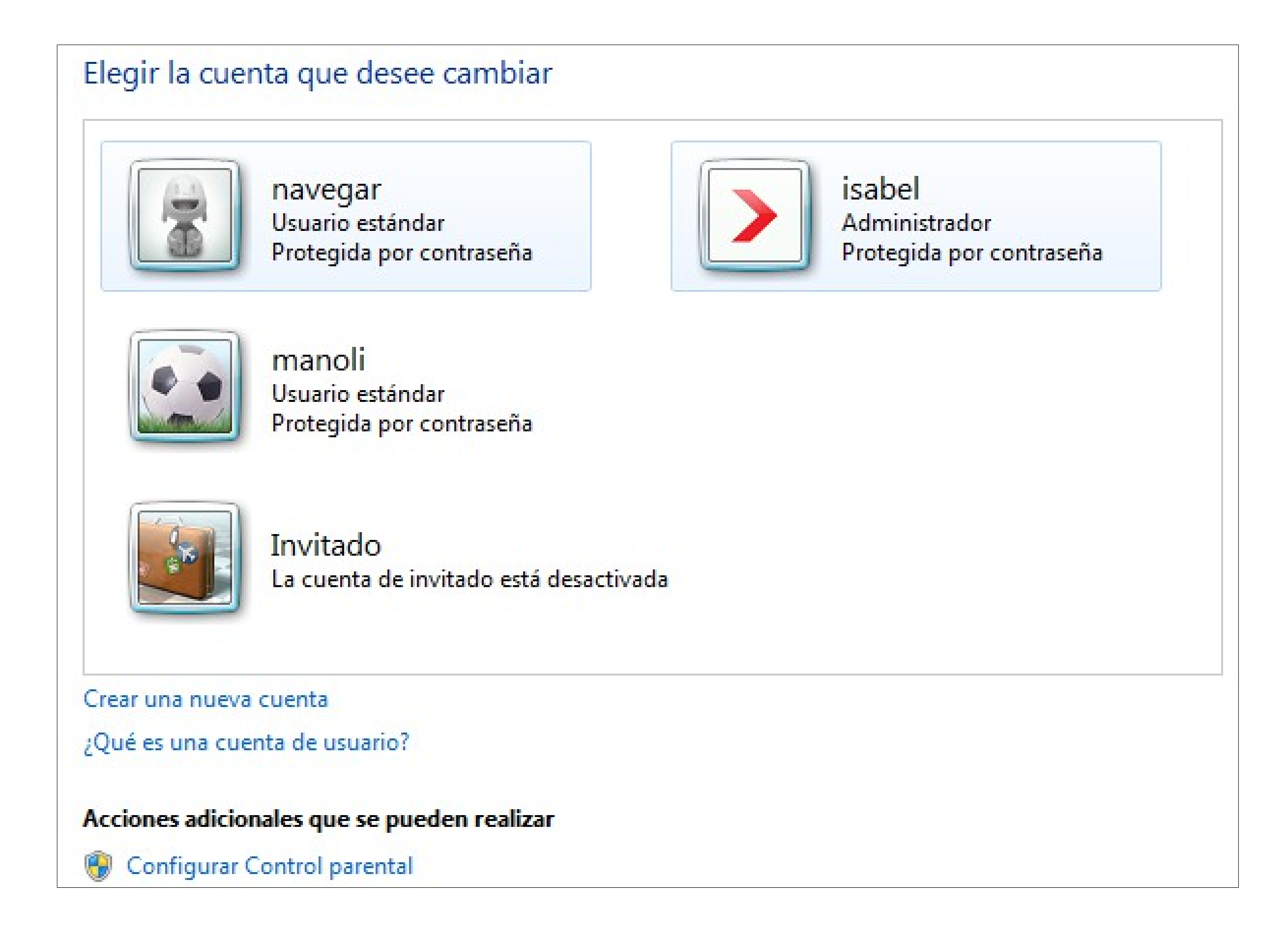
B. Quitar permisos a tu usuario habitual

Hacer clic en Inicio --> Panel de Control --> Cuentas de usuario

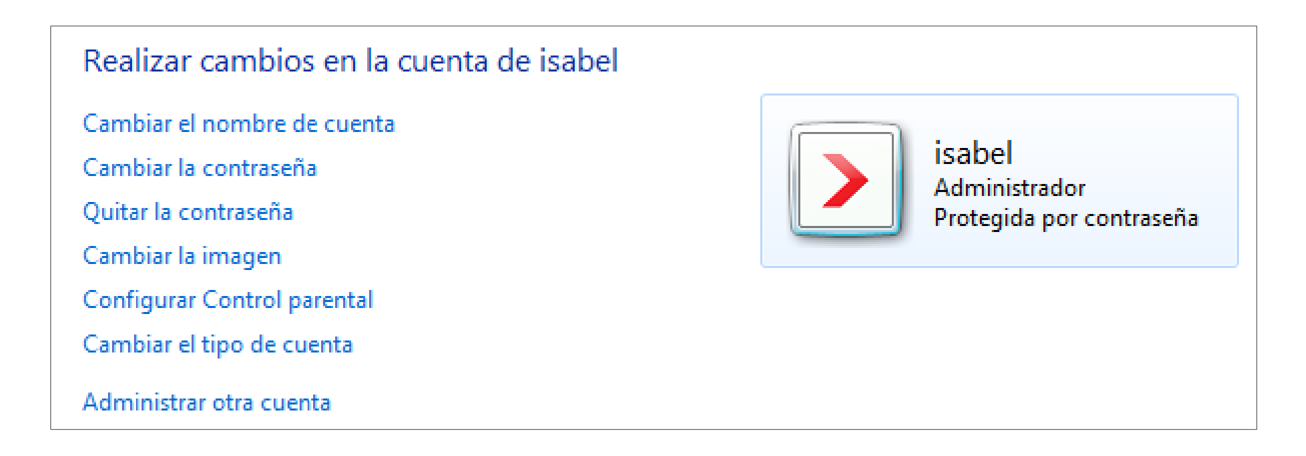
Hacer clic en “Agregar o quitar cuentas de usuario”



Elegir la cuenta que queremos cambiar

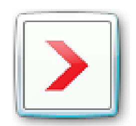


Hacer clic sobre Cambiar el tipo de cuenta.



Elegir usuario estándar y hacer clic sobre el botón cambiar tipo de cuenta.

Elija un nuevo tipo de cuenta para isabel



isabel
Administrador
Protegida por contraseña

Para poder cambiar este tipo de cuenta de usuario, debe asignar a otro usuario de este equipo una cuenta de administrador. Esto asegura que siempre habrá al menos un usuario con una cuenta de administrador de equipo en este equipo.



Usuario estándar

Los usuarios de cuentas estándar pueden usar la mayoría de software y cambiar la configuración del sistema que no afectan a otros usuarios ni a la seguridad del equipo.

Administrador

Los administradores tienen acceso completo al equipo y pueden hacer los cambios que deseen. Según la configuración de las notificaciones, es posible que se pida a los administradores que proporcionen su contraseña o una confirmación antes de realizar cambios que puedan afectar a otros usuarios.

Se recomienda proteger todas las cuentas con una contraseña segura.

¿Por qué se recomienda usar una cuenta estándar?



Cambiar el tipo de cuenta | Cancelar

Proteger las contraseñas

Actualmente, el método más extendido para obtener acceso a información personal que hemos almacenado en nuestro equipo y/o servicios en línea es mediante contraseñas.

La mayoría de las veces una contraseña es la única barrera entre nuestros datos confidenciales y los ciberdelincuentes.

Por lo que merece la pena invertir un poco de tiempo y esfuerzo para gestionarlas eficazmente.

1. **Elegir una contraseña robusta**

- No usar palabras que se puedan encontrar en un diccionario
- Usar una longitud de contraseña de 8 dígitos al menos.
- Combinar mayúsculas, minúsculas, números y símbolos.

2. **Protegerla bien**

- No dejar que los navegadores recuerden las contraseñas
- Cambiarla periódicamente
- No usar la misma contraseña en dos sitios distintos.

La elección de contraseñas seguras tiene dos inconvenientes : son difíciles de crear y de recordar.

A. El método de la frase.

E1ldlm,dcnnqa

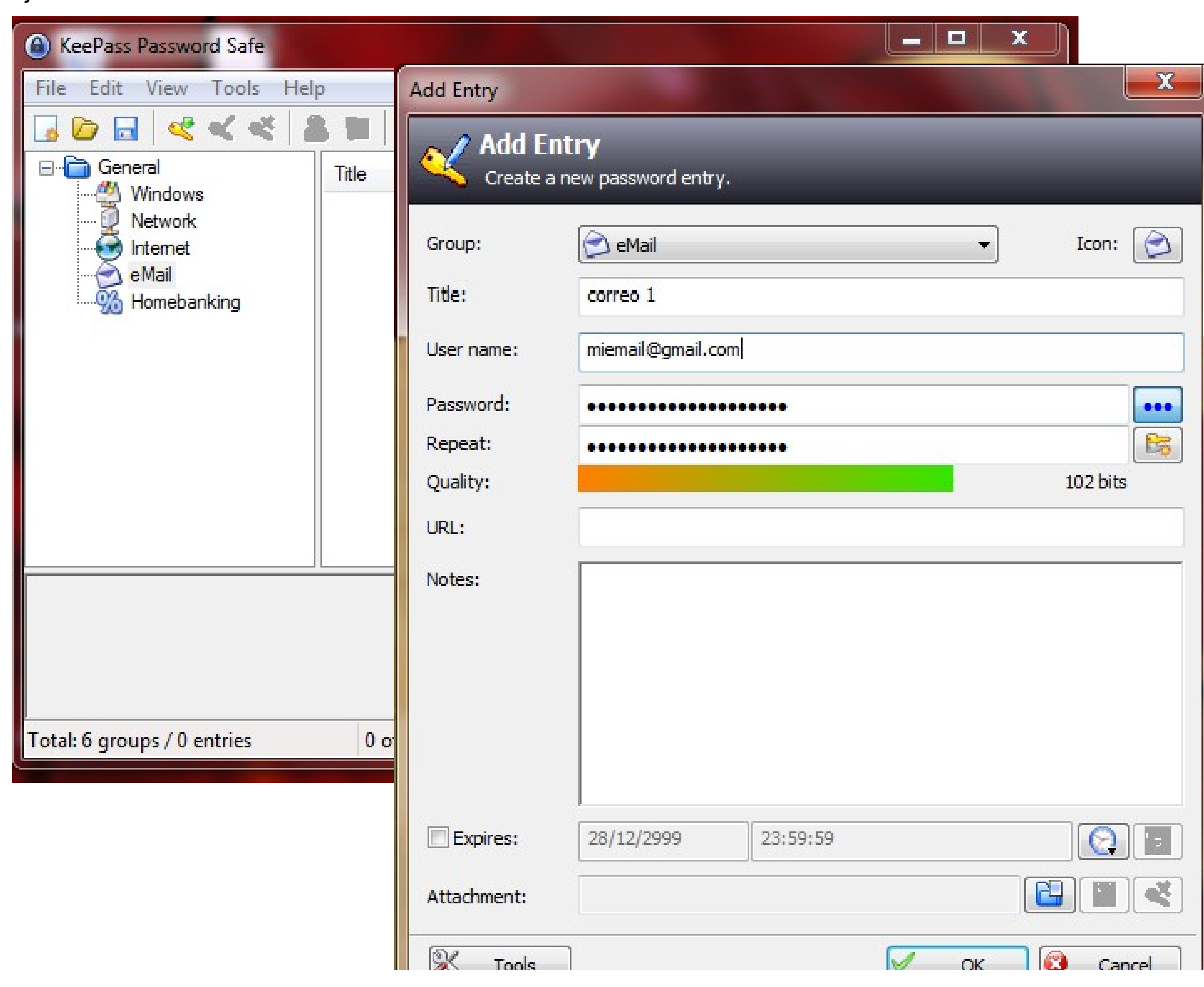
“En un lugar de la mancha, de cuyo nombre no quiero acordarme”

Elegir la frase de un libro, el título de una canción, la cita del día ...

B. Usar un gestor de contraseñas

Guarda las contraseñas encriptadas y las protege con una contraseña maestra

Ej: KeePass



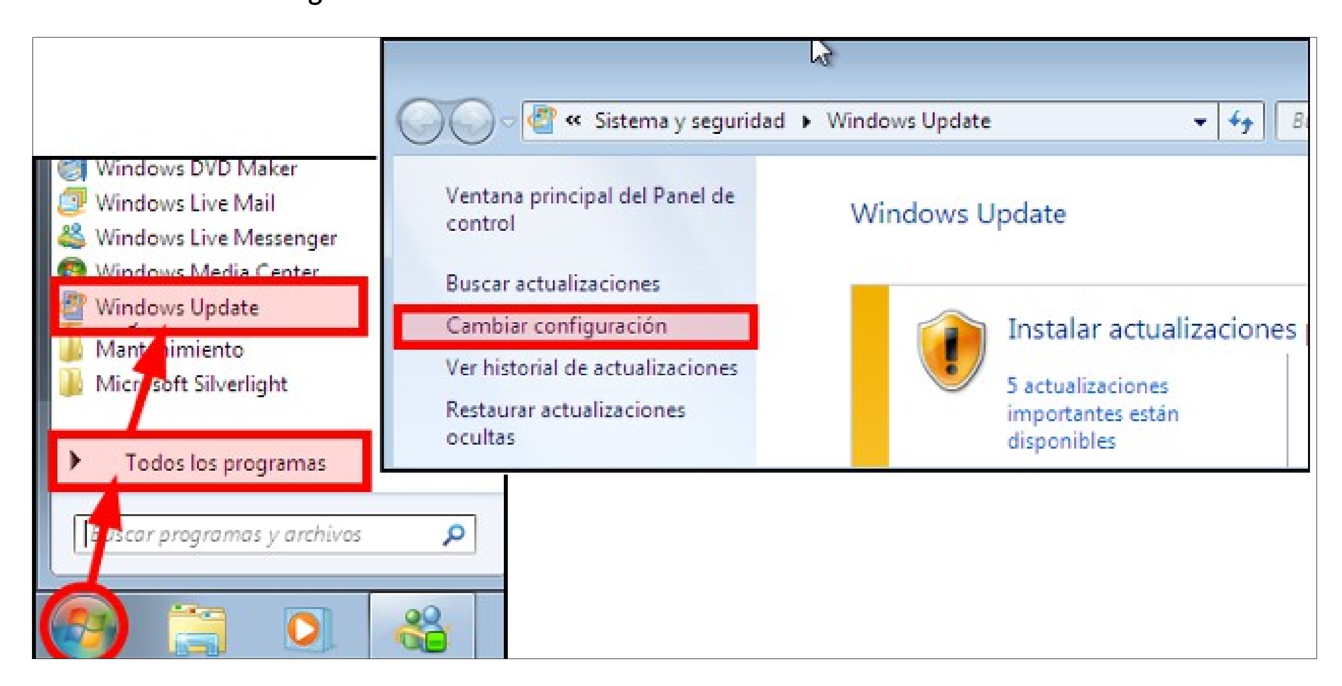
o guardar las contraseñas físicamente en un sitio seguro.

Desinstalar todos los programas que no necesites.

Mantener actualizados todos los demás

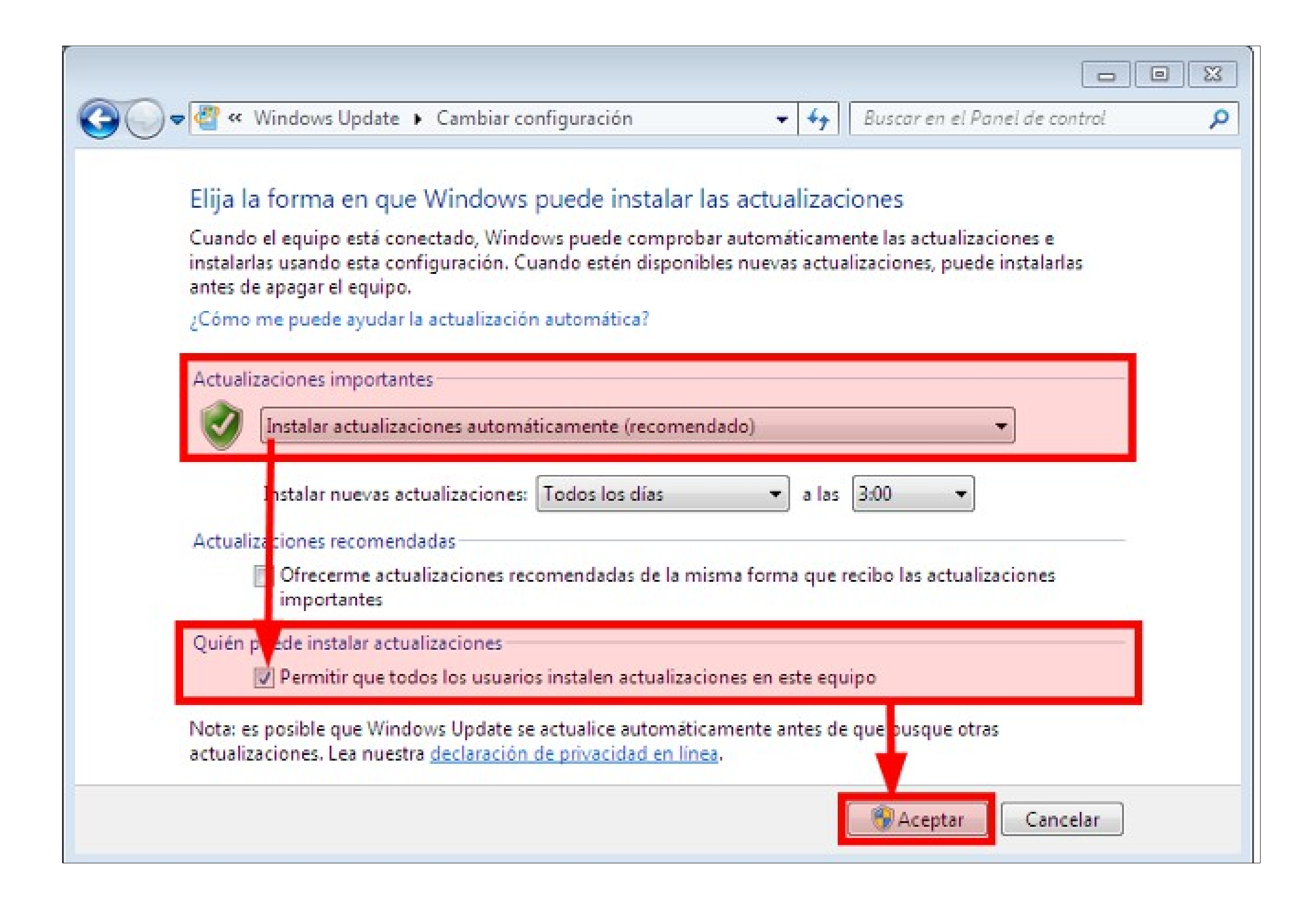
Windows 7

Pulsar en *Inicio → Todos los programas-> Windows Update*, en el panel izquierdo, pulsar en *Cambiar la configuración*.



Del desplegable de *Actualizaciones importantes*, seleccionar *Instalar actualizaciones automáticamente (recomendado)*, se marcará la opción *Permitir que todos los usuarios instalen actualizaciones en este equipo*.

Por último, hacer clic en el botón *Aceptar*



Actualización de java

Nota:

Es posible que tengas instalado el programa java en tu equipo y no lo necesites. Esto solo puedes comprobarlo, probando a desinstalar java y comprobando que puedes trabajar normalmente con tu equipo.

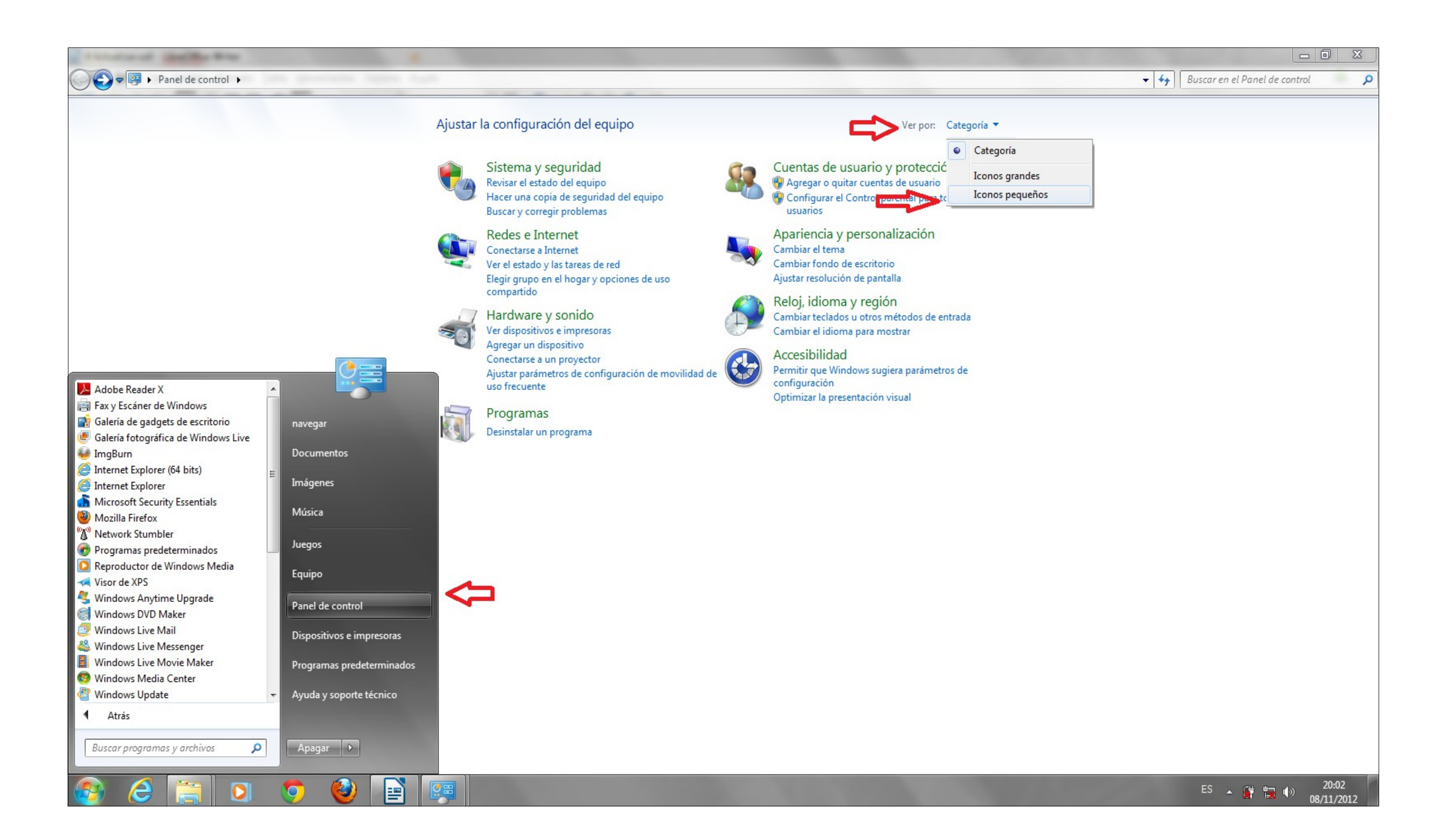
Si es así, es mucho más recomendable y más cómodo que desinstales java en vez de actualizarlo.

Para desinstalar java,

> Hacer clic en *Inicio → Panel de control → Desinstalar un Programa*
>
> En la lista de programas, seleccionar todas las versiones de java y hacer doble clic sobre cada una de ellas.
>
> Reiniciar el equipo

Para actualizar java

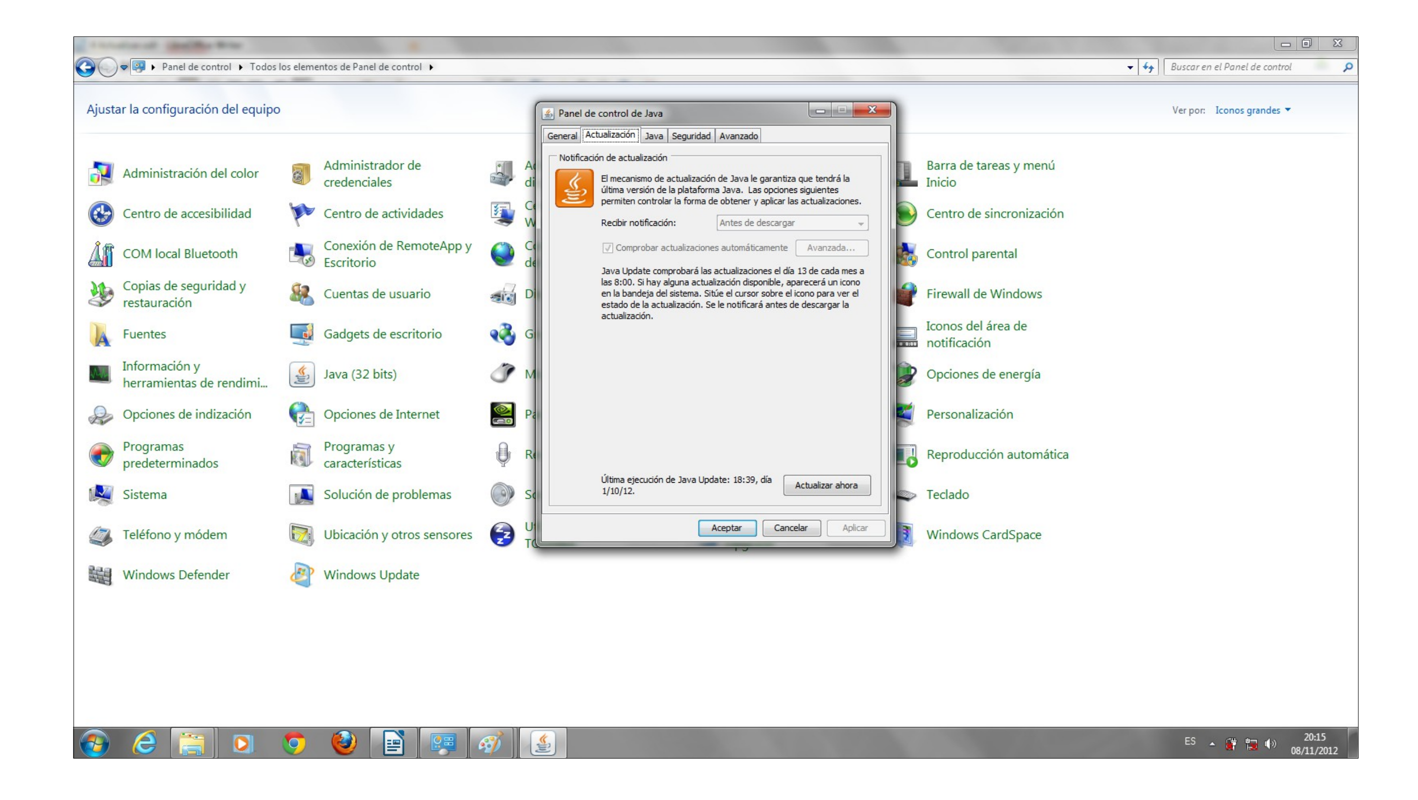
Hacer clic en *Inicio > Panel de control*



Hacer doble clic en el icono de *Java*. Aparece el Panel de control de Java.

Hacer clic en la ficha *Actualización*

Para activar la función Actualización de Java de modo que se compruebe automáticamente la existencia de actualizaciones, seleccione la casilla de verificación *Comprobar actualizaciones automáticamente*.

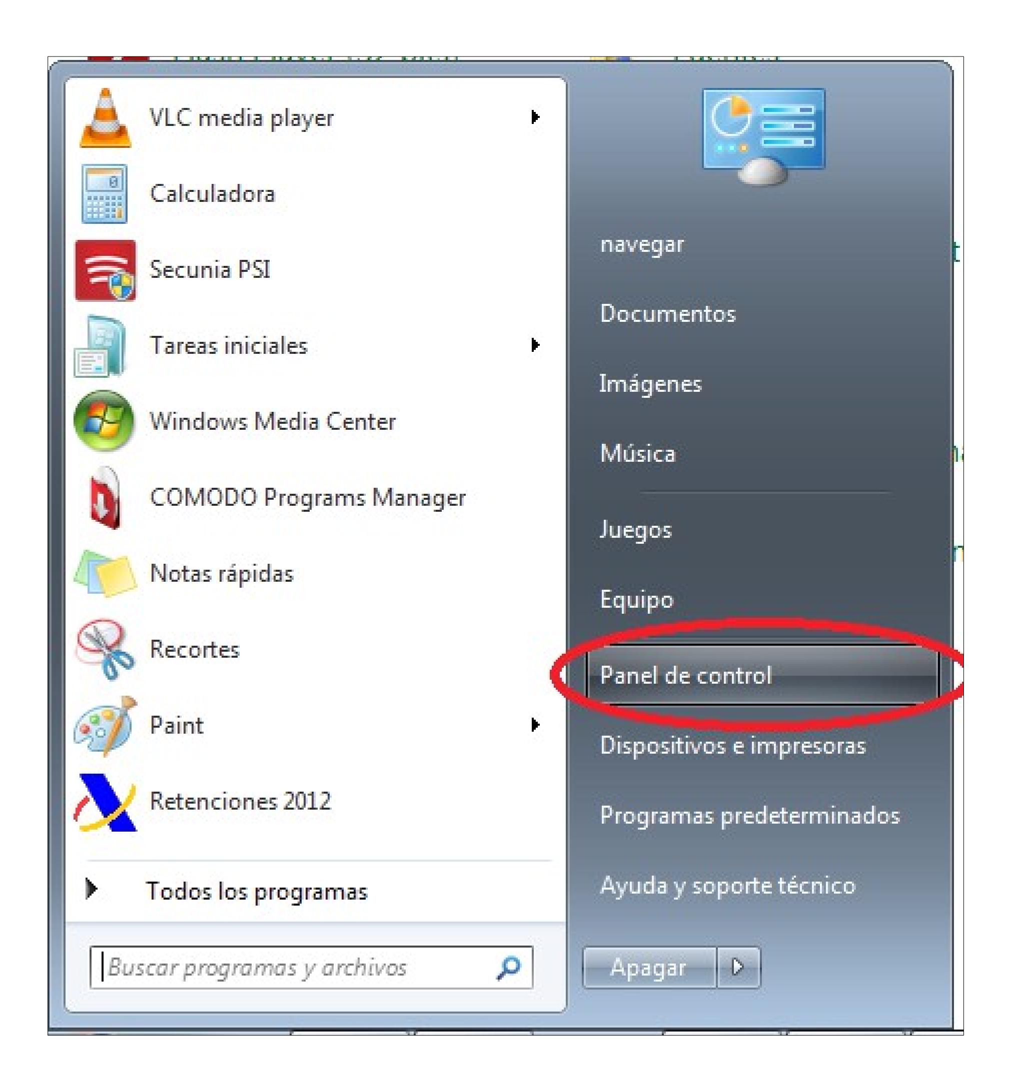


Una vez configurado esto, Java avisará cada vez que haya una actualización disponible.

Esta actualización se debe instalar en una cuenta con permisos de administración

Actualización Flash Player

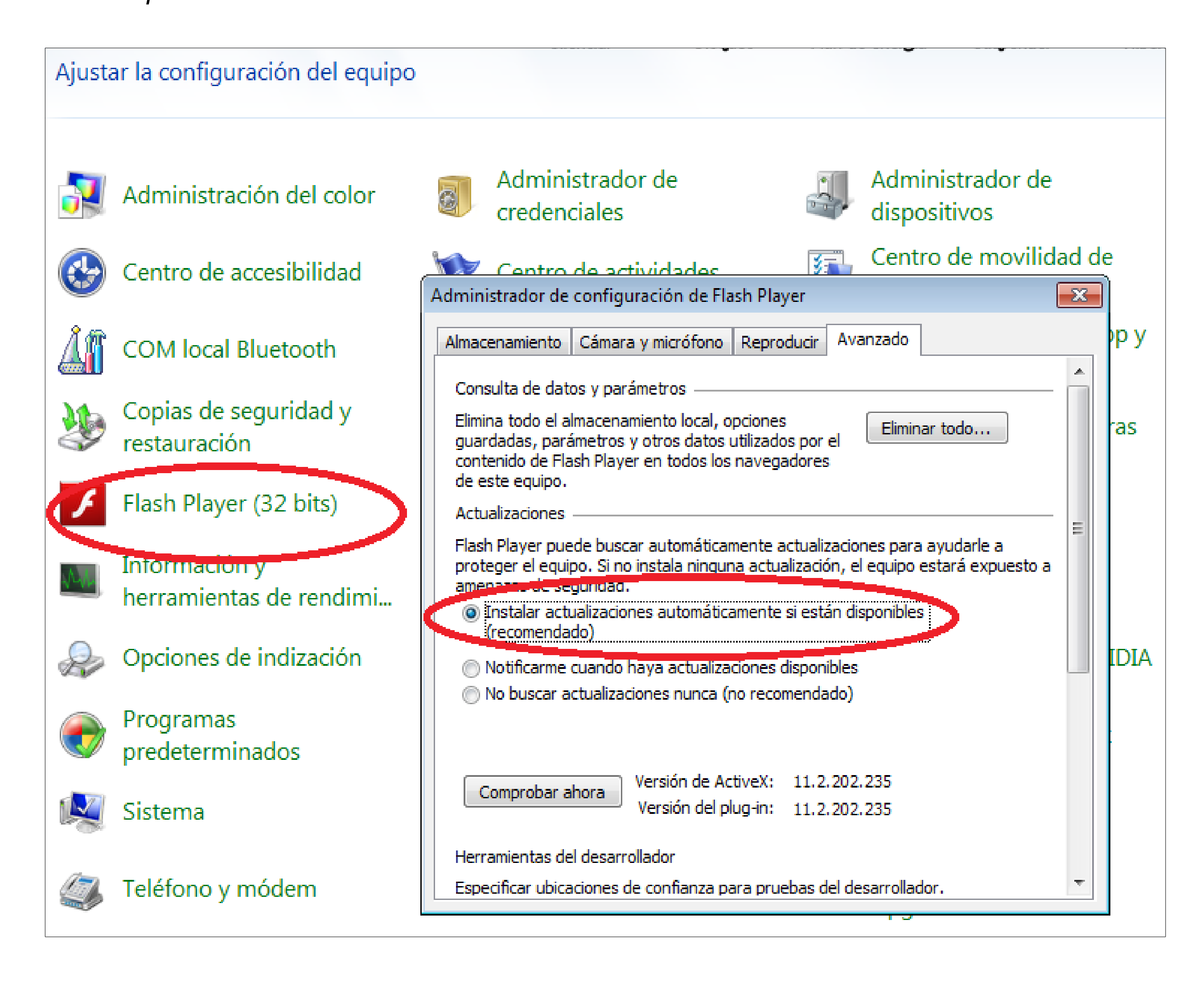
Hacer clic en *Inicio --> Panel de control*



Hacer doble clic en el icono de *Flash Player*. Aparece el Panel de control de Flash Player.

Hacer clic en la pestaña *Avanzado*.

Para activar la función Actualización de Flash de modo que se instalen automáticamente las actualizaciones, seleccionar la casilla *Instalar actualizaciones automáticamente si están disponibles.*



Normalmente vienen configurados para actualizarse automáticamente los siguientes programas

- Adobe Reader
- Firefox (y sus plugins)
- Chrome (y sus plugins)

Es importante aceptar sus peticiones de actualización

Un antivirus

La eficacia de los antivirus empieza en el 90% de detección, en algunos antivirus es más alta que en otros, pero nunca llega al 100%.

Existen diferentes tipos de antivirus, algunos son gratuitos y otros son de pago, pero, en mi opinión, no es necesario escoger ningún antivirus específico para estar seguros.

Lo importante es conseguir el antivirus de forma fiable(teniendo cuidado con el software que se instala. Instalar solo de sitios oficiales. No instalar software pirata.) y mantenerlo actualizado !

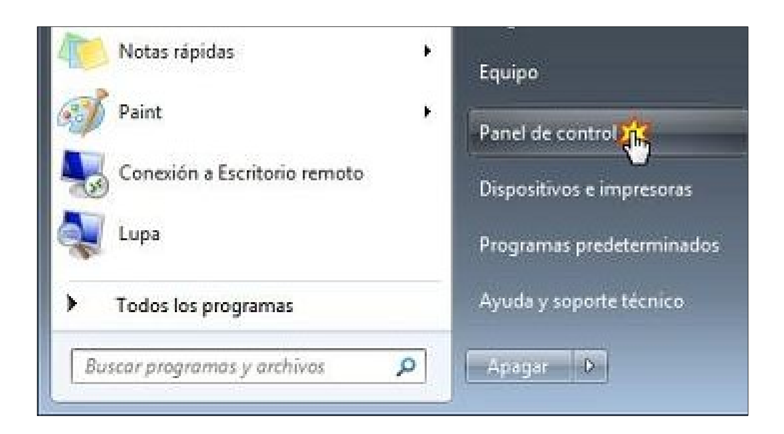
Ejemplos de antivirus fáciles de usar: Microsoft Security Essentials, Avast! ...

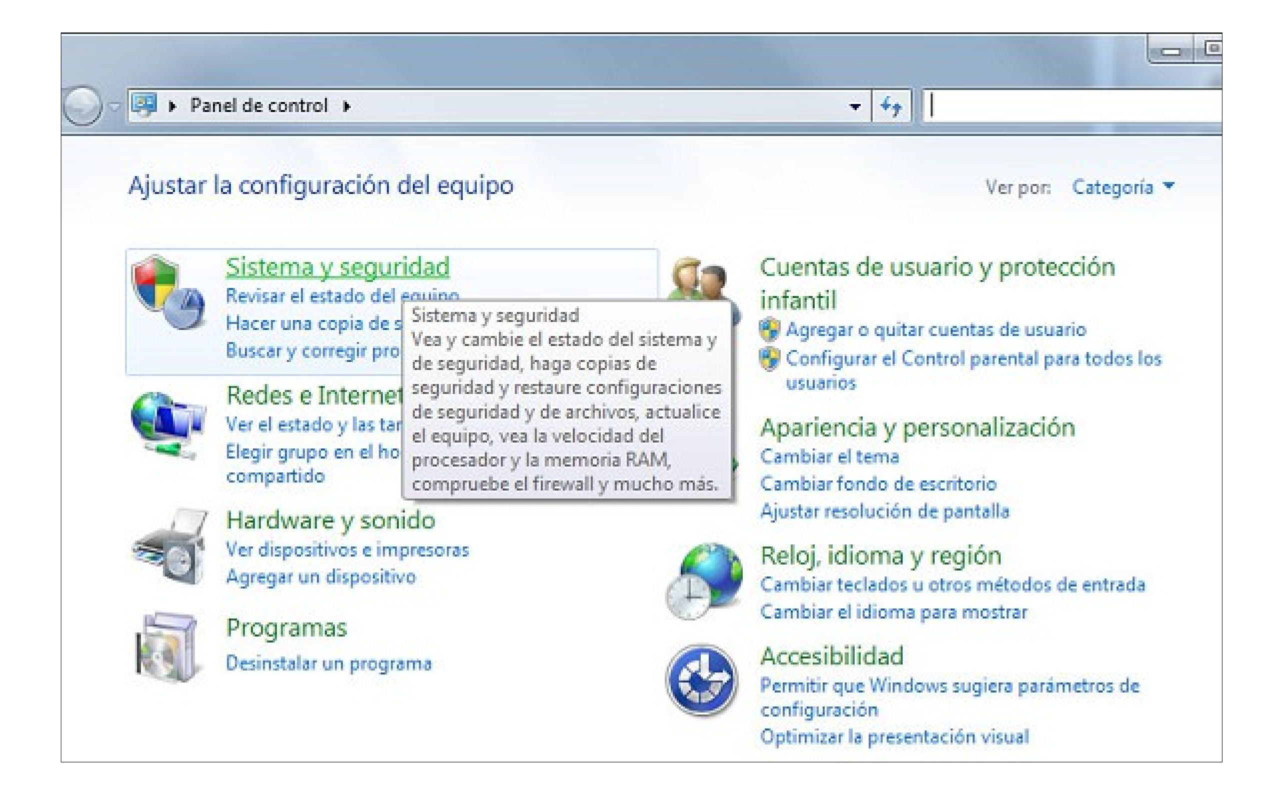
Un cortafuegos

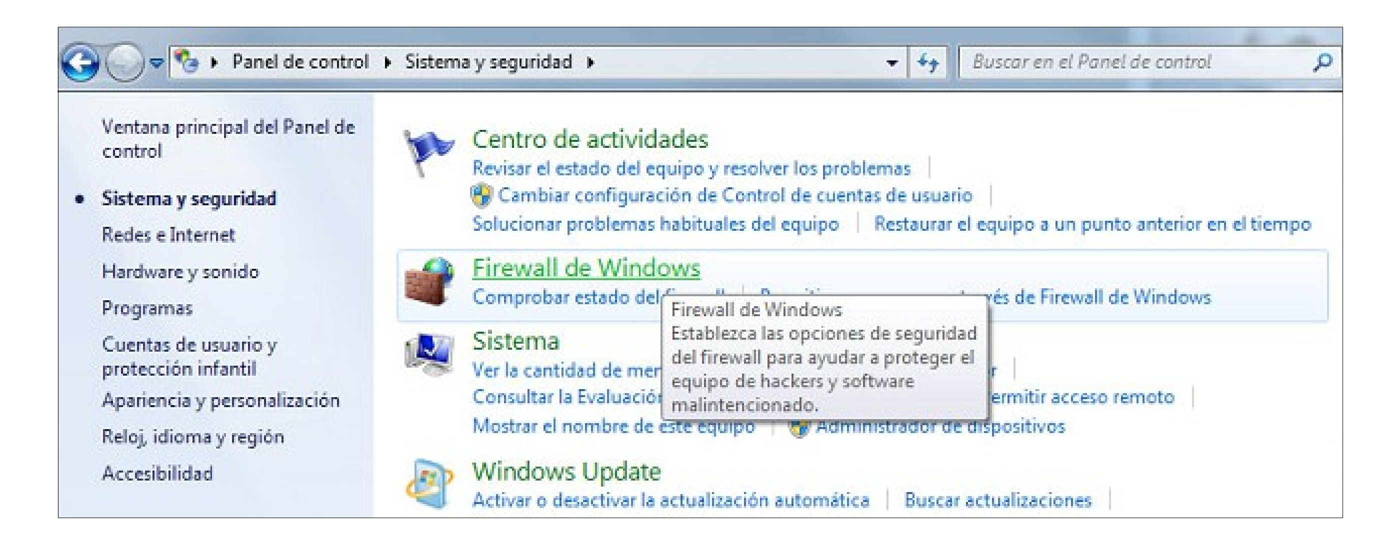
Exactamente igual que con los antivirus, los puntos importantes a la hora de usar un cortafuegos son que sea fácil de usar, conseguido por medios fiables y se mantenga actualizado.

Ejemplo de cortafuegos fácil de usar: Cortafuegos de Windows.

Para acceder a las opciones del cortafuegos hay que ir a Inicio -> Panel de Control -> Sistemas y Seguridad > Firewall de Windows, como se ve en las siguientes imágenes:

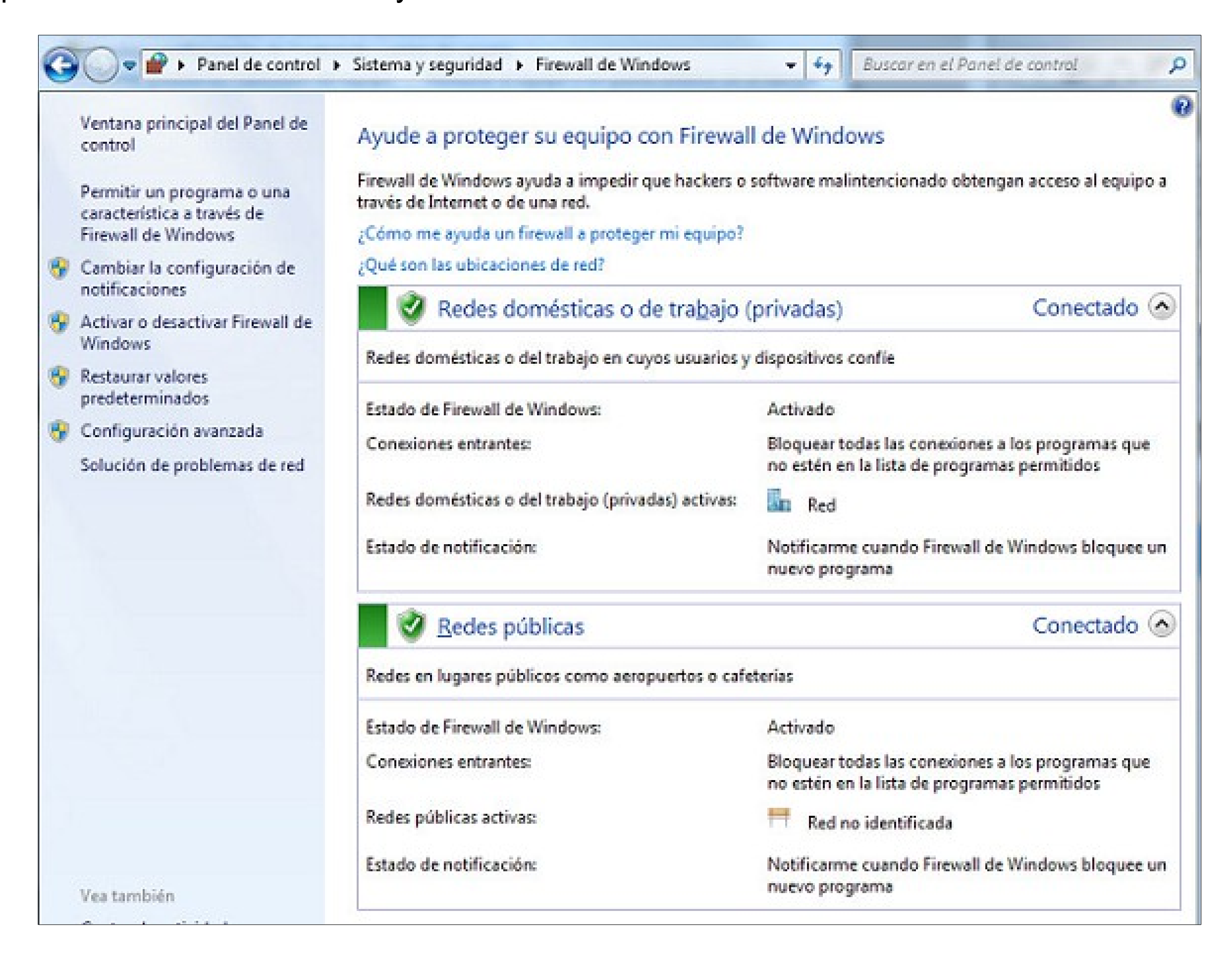






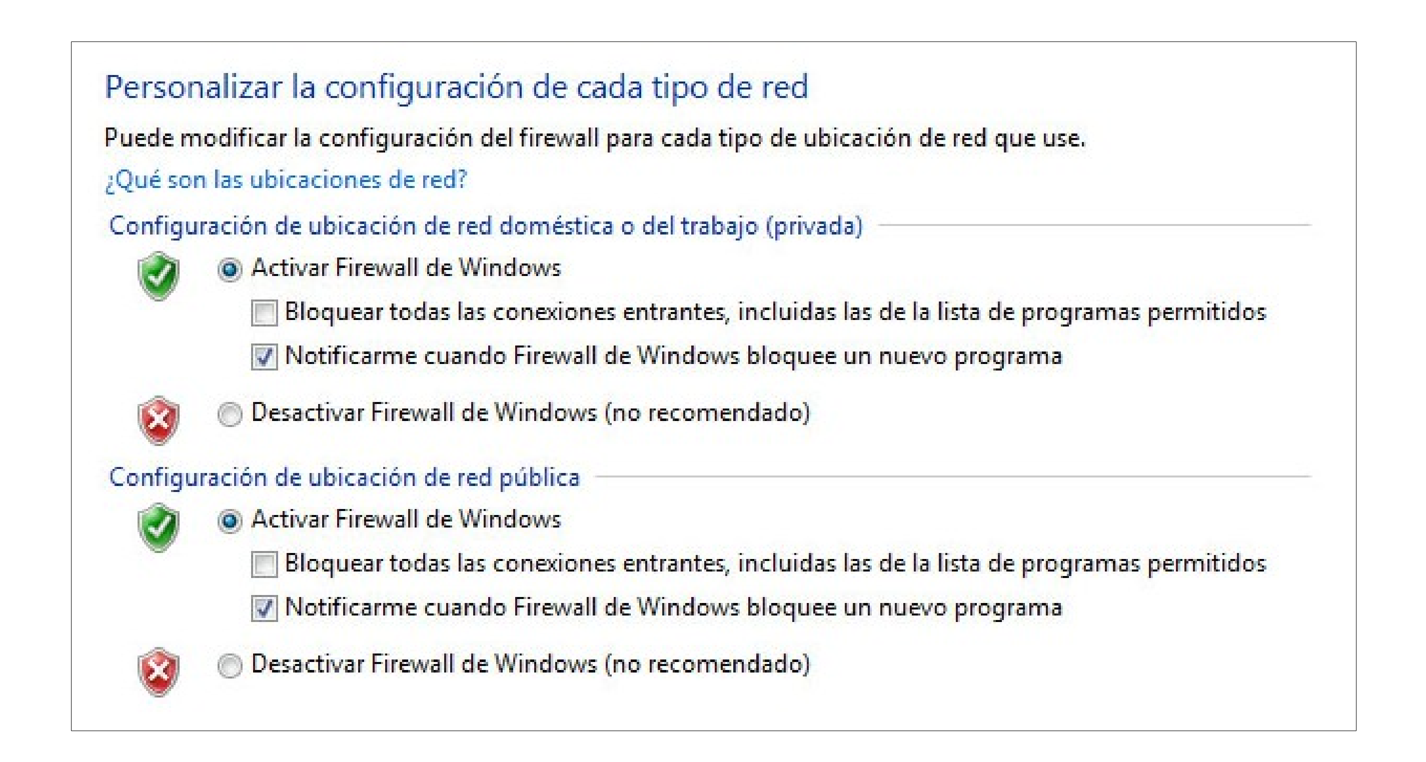
Si se realiza esta operación con una cuenta que no sea la de administrador, antes de poder ver las opciones del cortafuegos, aparecerá una ventana emergente de UAC -Control de Cuentas de Usuario, en la que habrá que confirmar que realmente se desea ejecutar el cortafuegos de Windows.

En la ventana del cortafuegos, lo primero que se muestra es si está habilitado para las opciones de Redes Privadas y Redes Públicas:



Es posible habilitar o deshabilitar el cortafuegos pulsando en la opción "Activar o desactivar cortafuegos de Windows" que hay en el menú izquierdo de la ventana.

No se debe habilitar la opción de "Bloquear todas las conexiones entrantes, incluidas las de la lista de programas permitidos", porque sería prácticamente lo mismo que no estar conectado a Internet.



Cada vez que un nuevo programa se quiera conectar a Internet, aparecerá un mensaje del cortafuegos de Windows preguntando si se desea permitir la conexión.

Referencias

1. CCN-CERT.INFORME DE AMENAZAS CCN-CERT IA-04/12. CIBERAMENAZAS 2011 Y TENDENCIAS 2012. Pag 104
2. EUROSTAT. http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-07022011-AP/EN/4-07022011-AP-EN.PDF. 21/02/2011
3. CCN-CERT.INFORME DE AMENAZAS CCN-CERT IA-04/12. CIBERAMENAZAS 2011 Y TENDENCIAS 2012 Pag 108
4. EUROSTAT. http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-07022011-AP/EN/4-07022011-AP-EN.PDF. 21/02/2011

Más Información

General

1. **Brigada de Investigación Tecnológica - Cuerpo Nacional de Policía**

Consejos de seguridad
http://www.policia.es/org_central/judicial/udef/bit_conse_segurid.html

2. Oficina de seguridad del internauta - Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información

http://www.osi.es

3. Banco de España - Finanzas para todos

http://www.finanzasparatodos.es/es/kitsupervivencia/protecciondatospersonales

Distribución Live de Linux

4. U.S Air Force Research Laboratory

http://www.spi.dod.mil/lipose.htm

Seguridad WiFi

5. Instituto de las Tecnologías de la Comunicación -Ministerio de Industria, Turismo y Comercio

http://cert.inteco.es/Proteccion/Configuraciones_seguras/WiFi/wifi_medidas_basicas/

No confiar en extraños

6. **WOT**

https://www.mywot.com/

7. Virus Total

https://www.virustotal.com/

Utilizar los mínimos permisos

8. Microsoft

http://windows.microsoft.com/es-ES/windows7/User-accounts-frequently-asked-questions

9. Oficina de seguridad del internauta

http://www.osi.es/cuentas-de-usuario/

Contraseñas

10. Oficina de seguridad del internauta

http://www.osi.es/contrasenas/

11. KeePassX

http://www.keepassx.org/

Actualizaciones de seguridad y desinstalar Java

12. Oficina de seguridad del internauta

http://www.osi.es/actualizaciones-de-seguridad/

13. Hispasec

http://unaaldia.hispasec.com/2012/08/si-no-actualizas-java-estas-infectado.html

http://unaaldia.hispasec.com/2012/04/una-vulnerabilidad-para-explotarlos.html

Antivirus

14. Av Comparatives

http://www.av-comparatives.org/comparativesreviews/dynamic-tests

15. Microsoft

http://windows.microsoft.com/es-ES/windows/security-essentials-download

16. Avast

http://www.avast.com/es-es/free-antivirus-download

Cortafuegos

17. Oficina de seguridad del internauta

http://www.osi.es/es/herramientas-gratuitas/firewall-de-windows

18. Microsoft

http://windows.microsoft.com/es-es/windows7/products/features/windows-firewall